UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/990,860 | 11/09/2001 | James W. Kasper | 062891.0668 | 2711 |

5073 7590 03/25/2005

BAKER BOTTS L.L.P.
2001 ROSS AVENUE
SUITE 600
DALLAS, TX 75201-2980

| EXAMINER | |
|---|---|
| ABYANEH, ALI S | |
| **ART UNIT** | **PAPER NUMBER** |
| 2133 | |

DATE MAILED: 03/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/990,860 | KASPER ET AL. | |
| | Examiner | Art Unit | |
| | Ali S. Abyaneh | 2133 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *09 November 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on *09 November 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *08-04-03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## Detailed ACTION

1. Claims 1-39 are presented for examination.

### *Information Disclosure Statement PTO-1449*

2. The Information Disclosure Statement submitted by applicant on 08/04/2003 has been considered. Please see attached PTO-1449.

### Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claim 1,2,5-10,35,36 are rejected under 35 U.S.C. 102(b) as being anticipated by Stephen E. Smaha et al. (US Patent NO.5, 557,742).

**Regarding Claim 1**

Smaha teaches a method for intrusion detection of network traffic comprising: storing a data file comprising data defining one or more signature definition and one or more parameters and associated values( column8, lines 8-36); generating, for each of the

one or more signature definitions, an inspector instance based on the data file; and executing, for each of the one or more signature definitions, the generated inspector instance to detect network traffic matching the signature definition (column 10, lines 10-45).

**Regarding Claim 2**

Smaha teaches a method comprising: storing user data file comprising signature definitions, each modified signature definition comprising signature identifier associating the modified signature definition with a corresponding signature definition stored in the data file. [(column 8, lines 8-36)(examiner considers signature data structure as applicant's signature definition and any element of signature data structure as applicant's identifiers)] and generating, for each of the modified signature definitions, revised inspector instance based the modified signature definition and corresponding generated inspector instance (column 10, lines 10-23).

**Regarding Claim 5**

Smaha teaches a method, wherein the one or more modified signature definitions comprises modified values for associated modified parameters and no values indicative of the parameters in the corresponding signature definition that are not modified. (column 8, lines 8-36).

**Regarding Claim 6**

Smaha teaches a method, wherein the data file comprises a file received from a

sensor provider [(column 9, lines 2-4) (examiner considers item 128 as applicant's sensor provider)].

**Regarding Claim 7**

Smaha teaches a method, wherein the data file comprises a file generated by a user (fig 1, item 22).

**Regarding Claim 8**

Smaha teaches a method, wherein receiving the datafile comprises receiving the data file at a sensor configuration handler. [(column 8, lines 10-13)(examiner considers load mechanism 102 as applicant's sensor configuration handler)].

**Regarding Claim 9**

Smaha teaches a method comprising receiving configuration data from a user and storing the received configuration data in a user data file(column 9, lines 1-13).

**Regarding Claim 10**

Smaha teaches a method comprising: storing a user data file comprising one or more user-defined signature definitions, each user-defined signature definition comprising a signature identifier not associated with any of the signature definitions in the data file (column8, lines 8-36); and generating, for each of the user-defined signature

definitions, an inspector instance based on the user defined signature (column 10, lines 10-23).

**Regarding Claim 35**

Smaha teaches a system for intrusion detection, comprising: a sensor for detecting possible network intrusions, the sensor comprising: at least one engine (column4, lines 61-67); and a means for storing default signatures and user-defined signatures for defining signatures to be detected by the at least one engine (column 8, lines 8-22 and column 10, lines 10-45).

**Regarding Claim 36**

Smaha teaches a method for use in intrusion detection of network traffic comprising: storing in a memory a signature definition associated with a signature to be detected, the signature definitions comprising: an identifier for the signature; and one or more parameter-value pairs associated with the signature, each parameter-value pair comprising a parameter name and associated parameter value [(column 8, lines 8-36)(examiner considers signature data structure as applicant's signature definition and elements of signature data structure as applicant's identifiers, parameters-value pairs, parameter name and associated parameter value)] ; and determining, based on the signature definition, the values that associated parameters of' network traffic must take to meet the signature (column10, lines 10-42).

## Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) patent may not be obtained though the invention is not identically disclose or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claim 3 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stephen E. Smaha et al. (US Patent NO.5, 557,742) in view of Brian D. Hanner (Publication NO.2003/0033435).

### Regarding Claim 3 and 39

Smaha teaches all limitation as applied to claim 1 and 36 above but he does not explicitly teach a method wherein the data file comprises, for each signature definition, data comprising: a signature identification number parameter and associated value; a signature name and associated string; one or more parameters and respective values defining characteristics of the signature and each signature definition further comprises an identification parameter preceding the signature identifier. However, in an analogous art, Hanner teaches a method wherein, the data file comprises, for each signature definition, data comprising: a signature identification number parameter and associated value; a signature name and associated string; one or more parameters and respective values defining characteristics of the signature and each signature definition further comprises an identification parameter preceding the signature identifier (paragraph

[0067] and [0068]). Therefore it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Smaha to include a signature identification number parameter and associated value; a signature name and associated string; and one or more parameters and respective values defining characteristics of the default signature. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to represent the data by collection of groups that comprise the signature, which convey all information necessary to determine final outcome.(paragraph [0039]).

7. Claims 4,11-16,19,20,23,24,26,27 and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stephen E. Smaha et al. (US Patent NO.5, 557,742) in view of Allen Gluck et al. (US Patent NO.5,948,104).

**Regarding Claim 4 and 37**

Smaha teaches all limitation of the claim as applied to claim 1 and 36 above but he does not explicitly teach a method wherein each signature definition and plurality of signature definitions are stored in a separate line of the data file. However, in an analogous art, Gluck teaches a method wherein each signature definition and plurality of signature definitions are stored in a separate line of the data file (column 5, lines 55-67). Therefore it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Smaha to store each

signature definition and plurality of signature definition in a separate line of data file. This modification would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to store signature according to ascending numerical order of the corresponding virus signatures(column6, lines 1-3).

**Regarding Claim 11**

Smaha teaches a method for use in intrusion detection comprising: storing a default signature file defining one or more default signatures (column 8, lines 8-22) ; automatically generating, for each of the one or more signatures defined in the default signature file, executable code operable to detect intrusions associated with the default signature ( column 10, lines 10-45). Smaha does not explicitly teach storing a customized signature file defining one or more custom signatures; and automatically generating, for each of the custom signatures, executable code operable to detect intrusions associated with the custom signature. However, in an analogous art, Gluck teaches a method, which updates the signatures, and automatically generating, for each of the custom signatures, executable code operable to detect viruses (intrusion) associated with the custom signature. [(column 7, lines 45-59) (examiner considers updated virus signature as applicant's custom signature )]. Therefore it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Smaha to include storing updated signature file defining one or more custom signatures; and automatically generating, for each of the custom signatures, executable

code operable to detect viruses associated with the updated signature. This modification would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to scan the system with the new virus detection and repair information (column 10, lines10-12).

**Regarding Claim 12 and 13**

Smaha teaches all limitation of the claim as applied to claim 10 above but he does not explicitly teach storing a customized signature file comprises storing modifications of one or more of the default signatures and automatically generating, for each of the one or more custom signatures comprises automatically generating, for each custom signature, executable code operable to detect intrusions associated with the custom signature based on the generated executable code of an associated default signature. However, in an analogous art, Gluck teaches a method, wherein storing a virus signature update file (customized signature file) comprises storing modifications of one or more of the default signatures. (column 8, lines 17-49) and automatically generating, for each of the one or more signature update (custom signatures) comprises automatically generating, for each signature update (custom signature), executable code operable to detect viruses (intrusions) associated with the signature update (custom signature) (column 5, lines 14-44) based on the generated executable code of an associated default signature. (column 2, lines 62-65 ).Therefore it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Smaha to include storing a signature update file (customized signature file) comprises storing modifications of one or more of the default signatures and automatically generating, for

each signature update (custom signature), executable code operable to detect viruses (intrusions) associated with the signature update (custom signature) based on the generated executable code of an associated default signature. (column 2, lines 62-65 ).This modification would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to update the signature files so that anti-virus program stored thereon will be able to detect and eliminate viruses including newly created ones.(column 2,lines 30-35).

**Regarding Claim 14**

Smaha and Gluck teach all limitation of the claim as applied to claim 11 above and furthermore Gluck teaches a method, wherein the one or more custom signatures comprises modifications of the default signatures.(column8, lines 20-49).

**Regarding Claim 15**

Smaha teaches a method, wherein generating, for each of the one or more default signatures, comprises generating executable code associated with the default signature based on an inspector shell [(column10, lines 10-45)(examiner considers transition function as applicant's inspector shell)].

**Regarding Claim 16**

Smaha teaches a method, wherein the executable code associated with the default signature is operable to compare a plurality of parameter values to a plurality of

parameter values defined by the default signature. [(column 6, lines 23-30 and column 10, lines 10-32) (examiner considers elements in event data structure as applicant's plurality of parameter values and elements of signature data structure as applicant's plurality of parameter values defined by the default signature)].

**Regarding Claim 19 and 23**

Smaha teaches a method for use in intrusion detection comprising: providing a sensor having a plurality of defined signatures, plurality of parameter names and associated value (column8, 8-19).Smaha does not explicitly teach communicating to the sensor a desire to create a modified signature from a signature to be modified; receiving from the sensor data indicative of parameters and associated values for the signature to be modified; providing to the sensor a modified value for at least one of the parameters to create a modified signature and modified signature comprises storing plurality of parameter names and associated value. However, in an analogous art, Gluck teaches a method wherein, communicating to the sensor a desire to create a modified signature from a signature to be modified; receiving from the sensor data indicative of parameters and associated values for the signature to be modified; and providing to the sensor a modified value for at least one of the parameters to create a modified signature and storing data associated with modified signature (column 8, lines 20-49). Therefore it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Smaha to include communicating to the sensor a desire to create a modified signature from a signature to be modified;

receiving from the sensor data indicative of parameters and associated values for the signature to be modified; providing to the sensor a modified value for at least one of the parameters to create a modified signature and storing plurality of parameter names and associated value for the modified signature. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to update signature files so that intrusion detection or anti virus program detect newly created viruses or intrusions.

**Regarding claim 20**

Smaha and Gluck teach all limitation of the claim as applied to claim 19 above and furthermore Gluck teaches a method comprising storing data associated with the modified signature in the sensor at a location separate from the associated unmodified signature (column 7, lines 55-59).

**Regarding claim 24**

Smaha and Gluck teach all limitation of the claim as applied to claim 19 above and furthermore Gluck teaches a method further comprising selecting a signature to be modified from the plurality of defined signatures.(column 8, lines 20-49).

**Regarding Claim 26**

Smaha and Gluck teach all limitation of the claim as applied to claim 19 above and furthermore Smaha teaches a method, wherein providing a sensor having a plurality

of defined signatures comprises providing a sensor having a default data file defining the defined signatures (column 8, lines 8-30).

**Regarding Claim 27**

Smaha and Gluck teach all limitation of the claim as applied to claim 26 above and furthermore Gluck teaches a method, comprising updating the default file (column 7, lines 54-59).

8. Claim 28,32-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stephen E. Smaha et al. (US Patent NO.5, 557,742) in view Phillip A. Porras et al. (US Patent NO.6, 321,338).

**Regarding Claim 28**

Smaha teaches a system for intrusion detection comprising: a sensor for detecting possible network intrusions (column 4, lines 61-67), and a configuration handler comprising: a default signature file storing one or more signature definitions defining one or more respective default signatures for use by the sensor; and a user signature file storing a plurality of user-defined signatures for use by the sensor(column8, lines 8-23); and wherein network detection engine is operable to generate an executable code based on either one of the stored default signatures or one of the stored user-defined signatures, the executable code operable to detect a network intrusion defined by the associated user-defined signature or the associated default signature.(Column 10, lines 1-54). Smaha

does not explicitly teach one or more engine groups each associated with one or more network detection engines. However, in an analogous art, Porras teaches one or more engine groups each associated with one or more network detection engines (column 4, lines 47-55). Therefor it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Smaha to include the plurality of engine groups. This modification would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to implement other forms of analysis (column 1, lines 66-67 and column 2, lines 1-7).

**Regarding Claim 32**

Smaha and porras teach all limitation as applied to claime 28 above and furthermore Smaha teaches a system, wherein the configuration handler further comprises a user interface operable to: provide a list of possible parameters for a particular engine; receive a plurality of values for one or more of the parameters to define a user-defined signature associated with the engine; and parameters; and write a user-defined signature to the user signature file (column 8, lines 8-41).

**Regarding Claim 33**

Smaha in view of porras teach all limitation as applied to claim 28 above and furthermore Smaha teaches a system, wherein the configuration handler further comprises a reader and dispatcher operable to read data from the default signature file

and user- signature file and transmit the read data to the one or more engine groups (column 8, lines 1-8-29 and column 9, lines 31-45).

**Regarding Claim 34**

Smaha in view of porras teach all limitation as applied to claim 28 above and furthermore Smaha teaches a system comprising management console associated with the sensor and operable to communicate configuration data to the configuration handler and receive configuration help [(column4, lines 44-49)(examiner considers input 20 as applicants management console)].

9. Claim 29-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stephen E. Smaha et al. (US Patent NO.5, 557,742) in view Phillip A. Porras et al. (US Patent NO.6, 321,338) and further in view of Allen Gluck et al. (US Patent NO.5,948,104).

**Regarding Claim 29, 30 and 31**

Smaha and Porras teach all limitation as applied to claim 28 above and furthermore Smaha teaches a configuration handler [(column 8, line 8-19 (examiner considers load mechanism 102 as applicant's configuration handler)];configuration handler furthercomprises a user interface operable to: receive an identification of a signature to be modified and parameters and associated values for the signature (column 8, lines 8-36) but they do not explicitly disclose configuration handler comprising stored

modification to the default signature, stored modification are stored in the user signature file, a list of parameters and associated values for the signature to be modified, receive revised values for one or more of the parameter and write a revised signature to the user-defined data file. However, in an analogous art, Gluck teaches a method comprising stored modification to the default signatures (column7,lines 54-59) and stored modifications are in the user signature file [(column 8, lines 40-45)(examiner considers virus signature files 110 as applicant's user signature file)] and a list of parameters and associated values for the signature to be modified; receive revised values for one or more of the parameter; and write a revised signature to the user-defined data file( column 8, lines 20-49).Therefor it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Smaha and Porras to include stored modifications to the default signatures , store the stored modifications in the user signature file, provide a list of parameters and associated values for the signature to be modified, receive revised values for one or more of the parameter and write a revised signature to the user-defined data file . This modification would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to update and add new virus signatures and detect new viruses.

10. Claim 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stephen E. Smaha et al. (US Patent NO.5, 557,742) in view of Allen Gluck et al. (US

Patent NO.5,948,104) and further in view of Brian D. Hanner (Publication NO.2003/0033435).

**Regarding Claim 17**

Smaha and Gluck teach all limitation of the claim as applied to claim 11 above but they do not explicitly teach default signature file comprises, for each default signature; a signature identification number parameter and associated value a signature name and associated string; and one or more parameters and respective values defining characteristics of the default signature . However, in an analogous art, Hanner teaches a method wherein, default signature file comprises, for each default signature; a signature identification number parameter and associated value a signature name and associated string; and one or more parameters and respective values defining characteristics of the default signature (paragraph [0067] and [0068]). Therefore it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Smaha and Glouck to include a signature identification number parameter and associated value a signature name and associated string; and one or more parameters and respective values defining characteristics of the default signature. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to represent the data by collection of groups that comprise the signature, which convey all information necessary to determine final outcome. (paragraph [0039]).

**Regarding Claim 18**

A custom (updated) signature can have the same characteristics and values as default signature. Therefore claim 18 is rejected for the same reasons as applied to claim 17.

**Regarding claim 21**

Smaha and Gluck teach all limitation of the claim as applied to claim 20 above including one or more parameters and associated values, but they do not explicitly teach storing in the sensor the name, signature identification number, and one or more parameters and associated values for the modified signature . However, in an analogous art, Hanner teaches a method of storing in the sensor the name, signature identification number, and one or more parameters and associated values for the modified signature (paragraph [0067] and [0068]). Therefore it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Smaha and Gluck to include storing in the sensor the name, signature identification number, and one or more parameters and associated values for the modified signature This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to represent the data by collection of groups that comprise the signature, which convey all information necessary to determine final outcome.(paragraph [0039]).

11. Claim 22 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stephen E. Smaha et al. (US Patent NO.5, 557,742) in view of Allen Gluck et al. (US Patent NO.5,948,104). And furthere in view of Alfonso De Jesus Valdes et al. (US Publication NO. 2002/0059078)

**Regarding claim 22**

Smaha and Gluck teach all limitation of the claim as applied to claim 19 above, including signature modification (column 8, lines 30-36) but they do not explicitly teach communicating to the sensor the name of an engine associated with the signature. However, in an analogous art, Valdes teaches communicating to the sensor the name of an engine associated with the signature (paragraph [0119]). Therefore it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Smaha and Gluck to include communicating to the sensor the name of an engine associated with the signature. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order for the sensors to monitor different aspects of a computer network, such as a sensor that monitors network traffic and a sensor that discovers and monitors available network resources (paragraph [0009]).

**Regarding claim 25**

Smaha , Gluck and Valdes teach all limitation of the claim as applied to claim 22 above and furthermore Gluck teaches a method comprising receiving a list indicative of all defined signatures associated with the engine (column 3, lines 62-67 ).

12. Claim 38 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stephen E. Smaha et al. (US Patent NO.5, 557,742) in view of Allen Flint et al. (US Patent NO.6,735,700).

**Regarding claim 38**

Smaha teaches all limitation of the claim as applied to claim 36 above, but he does not explicitly disclose a method, wherein each signature definition further comprises an engine parameter and an associated name for the engine parameter. However, in an analogous art, Flint teaches a method comprising an engine parameter and an associated name for the engine parameter (column 11, lines 41-45). Therefore it would have been obvious for person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Smaha to include an engine parameter and an associated name for the engine parameter. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to identify the context information to be included in the session stamp (column 11, line 60-65).

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

1. U.S.Patent No.6, 725,377

This reference relates to a method and a system for updating anti intrusion software.

2. U.S.Patent No. 6,681,331

This reference relates to detecting the use of the software, and more specially, to the dynamic detection of an intrusive anomalous use of the computer software.

3. U.S. Publication No. 2002/0157020

This reference relates protecting the core database from being accessed by malicious.

4. U.S. Publication No. 2003/0182414

This reference relates to updating of digital information sequences that comprise software, devices and data.

## Conclusion

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ali Abyaneh whose telephone number is (571) 272-7961. The examiner can normally be reached on Monday-Friday from (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert

Decady can be reached on (571)272-3819. The fax phone numbers for the organization where this application or proceeding is assigned as (703) 872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ali Abyaneh A.A
Patent Examiner
Art Unit 2133
March 3, 2005

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100